Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Information Security Policy

I. **Statement**

The Information Security Policy establishes the *minimum* benchmark to protect the security of State information assets through a layered structure of overlapping control and monitoring.

II. **Purpose**

State information is a valuable asset that must be secure, both at rest and in transit, and protected from unauthorized use, disclosure, modification, and destruction. Appropriate controls and procedures must be instituted to ensure that its confidentiality, integrity, and availability are not compromised.

III. **Applicability**

This Information Security Policy applies to:

1. The Executive Branch and *Semi-autonomous State Agencies*[1], irrespective of where their information assets are hosted; and
2. Information assets from other State government branches that are hosted by OIT, or those that traverse the State's wide area network.

IV. **Responsibilities**

A. The *Chief Technology Officer* executes this Policy for all information assets.

B. The *Enterprise Security Officer* owns, interprets, and enforces this Policy.

C. The *Agency Data Custodian*[2] executes this Policy for all information assets under their purview.

V. **Directives**

1. Non-State Access: OIT is responsible for analyzing the security risks whenever non-State entities access State information, and ensuring that such access is in full compliance with ALL existing OIT policies, practices, and procedures.

[1] See Definition[2]
[2] See Definition[1]

Any contract with a non-State entity involving access to State information assets must include an explicit provision binding the non-State entity to full compliance with ALL existing OIT policies, practices, and procedures.

Non-State access privilege must be just adequate enough to accomplish a narrowly-defined business mission, and no higher. The burden of justification rests entirely on the Agency Data Custodian, who is responsible for applying to the Enterprise Security Officer for said access. Said access is contingent upon explicit approval from the Enterprise Security Officer, and is subject to revocation by the Enterprise Security Officer at any time. It remains the burden of the Agency Data Custodian to apprise the Enterprise Security Officer re: any change in business requirement and/or the status of the non-State entity. Any non-State access will commence as late as practically possible and will terminate as soon as the underlying business requirement ceases to exist.

2. Data Classification: Agency Data Custodians must collaborate with the Enterprise Security Officer in adopting and adhering to an information classification system, the purpose of which is to ensure that all information assets are operated in a manner compliant with any and all applicable State and Federal regulations.

   High Risk: Information assets for which there exist legal regulations and/or penalties for disclosure. Data covered by Federal and State legislation, such as FERPA, HIPAA, IRS 1075, or the Data Protection Act, are in this class. In general, health, payroll, personnel, and financial data belong in this class. Other data included in this class include information that, if compromised, would cause severe damage to the State. The Agency Data Custodian makes this determination.

   Restricted: Data that may not cause severe damage to the State if it were to be compromised, but the Agency data custodian still desires to protect against unauthorized disclosure and/or modification. Again, the Agency Data Custodian makes this determination.

   Public: Information that may be freely disseminated.

   a. Agency Data Custodians must determine the data classification and must ensure that said data is protected in a manner commensurate with its classification.
   b. No information asset must be exposed to the Internet without the means to protect it in a manner commensurate with its classification.
   c. Both High Risk and Restricted data must be encrypted during transmission over insecure channels.

3. Education & Training: Information security training must be conducted and documented annually for all Agency personnel. Such training must include security awareness, updates to security policies or procedures, and reporting of incidents and vulnerabilities.

4. Incident Reporting: OIT will maintain a security incident reporting process and train its personnel, and at the request of an Agency, provide the same training to Agency

personnel. This process will allow OIT to document and monitor security incidents for commonalities, improve internal controls, and develop steps to remediate and reduce future security risks.

5. Discipline: State and Agency-specific discipline will be executed against users who violate this Policy.

6. Physical Security: Both OIT and Agencies must institute appropriate measures to prevent and detect unauthorized access or damage to facilities that contain State information assets. Facilities that house State information infrastructure assets must utilize physical access controls designed to permit access by authorized users only.

7. Infrastructure Protection: State information infrastructure assets must be protected from physical and environmental threats.

8. Power Supplies: Continuity of power must be provided to all critical State information infrastructure assets.

9. Malwares:
    a. Awareness, prevention, detection, and neutralization controls must be utilized to protect State information assets against malwares (rogue applications that disrupt the normal functioning of computers).
    b. Willful introduction of malwares into the State network is prohibited.
    c. Any and all devices that connect to the State network must be protected with an approved, licensed anti-malware that it is kept updated according to the anti-malware vendor's recommendations.
    d. All State information infrastructure assets must be hardened, and logs monitored, to protect against malwares.

10. Backup: Backups of all State information assets must be routinely created and properly stored to ensure prompt restoration, when necessary. Backups must be handled with exactly identical care and precaution as the original information asset itself.

11. Activity Logs: Logs of activities involving State information assets must be maintained and reviewed on a regular basis.

12. Storage Media Disposal: When no longer required, ALL storage media (both fixed and removable) must be permanently scrubbed or destroyed or rendered unrecoverable in accordance with applicable State, Federal, or Agency regulations.

13. Operational System Documentation: Operational system documentation for State information assets must be protected from unauthorized access.

14. Information Exchange Agreements: Specific agreements enforcing appropriate information security controls must be instituted for any information exchange among Agencies, as well as other external entities.

15. Electronic Commerce: State information accessed via electronic commerce must have appropriate security controls implemented based on the classification of the underlying data.

16. Email: OIT must administer a central email application, and acceptable use policies for the use of said email, complying with appropriate State and Federal regulations.

17. Access Control: Access to State information assets must be based upon each user's access privileges. Access privileges shall be granted on the basis of specific business need (i.e. need to know). When necessary, access may also be restricted by day, date, and time, as appropriate.

18. Access Authorization: Access to any State information asset must be authorized by the Agency Data Custodian.

19. Access Rights Review: Periodic log reviews of user access and privileges must be performed by the Agency Data Custodian in order to monitor access to State information assets, as well as deviations from authorized usage.

20. Passwords: Access to any State information asset must be through individual and unique logins, and must require authentication. Authentication includes the use of passwords, smart cards, biometrics, challenge-response questionnaire, or such other industry-accepted best practices. Users must select, employ, and manage passwords to protect against unauthorized discovery or usage. All users of high risk or restricted data must have a strong password, the definition of which will be established and documented by OIT, taking into account such features as length, complexity, unpredictability, expiration frequency, etc. Credentials for empowered accounts (such as administrator, root, or supervisor) must be changed frequently, consistent with guidelines established by OIT. Credentials for empowered accounts must be modified any time the underlying system is installed, rebuilt, or reconfigured. Service accounts that do not allow login are not considered empowered accounts. All default passwords must be modified immediately post-installation. Passwords must never be stored or transmitted without first having been hashed or encrypted.

21. Password Management System: Password management systems must be deployed to provide a reliable, effective method of ensuring strong passwords, as established and documented by OIT, taking into account such features as length, complexity, unpredictability, expiration frequency, etc.

22. Session Timeout: Agency Data Custodians must establish a standard length of inactivity time that will trigger a session to terminate in their respective Agencies. Any session that exceeds the preset timeout will either log off the user or lock the session until fresh re-authentication.

23. System Utilities: System utilities will be made available only to those who have a legitimate business case for a specific utility.

24. Operating Software and Source Libraries: The operating system files and application software, as well as program source libraries must be secured from unauthorized use or access.

25. Documentation: All information products must include sufficient documentation to satisfy any applicable audit and security policy requirements.

26. Mobile Computing: Agencies must comply with the Remote Access methods provided by OIT when remotely accessing the State network.

27. Teleworking: Where Agencies approve teleworking for their personnel, they must ensure that the security of State information assets is not compromised.

28. Application Input/Output Validation: Given the wide prevalence of injection vulnerabilities of applications, all applications must thoroughly validate their inputs to guard against attack vectors, and their outputs to guard against divulging backend details.

29. Internet Connectivity:
    a. All systems connected to the Internet must maintain a vendor-supported version of the operating system.
    b. All systems connected to the Internet must be current with all security patches.
    c. All connections to the Internet must go through a properly secured access point provided by OIT to ensure that the State network is protected.

VI. **Definitions**

1. Agency Data Custodian: Agency official, who, by virtue of their position, is the fiduciary owner of specific Agency information assets. Thus, for instance, the Director of the Labor Bureau of Unemployment Compensation (or their designee) is the Agency Data Custodian for Unemployment Compensation information assets, and the Director of the Health & Human Services Office of Family Independence (or their designee) is the Agency Data Custodian for Benefits information assets.

2. Semi-autonomous State Agency: An agency created by an act of the Legislature that is not part of the Executive Branch. This term does not include the Legislature, the Judiciary, the Office of the Attorney General, the Office of the Secretary of State, the Office of the State Treasurer, and the Audit Department.

VII. **References**

1. Application Deployment Certification Policy[3]

2. Infrastructure Deployment Certification Policy[4]

3. Remote Hosting Policy[5]

4. Policy to Safeguard Information on Portable Computing and Storage Devices[6]

VIII. **Document Information**

Initial Issue Date: May 1, 2012
Latest Revision Date: November 5, 2014 – to update enforcement.

Point of Contact: Henry Quintal, Architecture-Policy Administrator, OIT (207) 624-8836.

Approved By: James R. Smith, Chief Information Officer, OIT, (207) 624-7568.

Position Title(s) or Agency Responsible for Enforcement: Kevin St. Thomas, Enterprise Security Officer, OIT, (207) 624-9845.

Legal Citation: 5 M.R.S.A. Chapter 163 Section 1973 paragraphs (1) B and (1) D, which read in part, "The Chief Information Officer shall:" "Set policies and standards for the implementation and use of information and telecommunications technologies…" and "Identify and implement information technology best business practices and project management."

Waiver Process: See the Waiver Policy[7].

[3] http://www.maine.gov/oit/policies/Application-Deployment-Certification.htm
[4] http://www.maine.gov/oit/policies/Infrastructure-Deployment-Certification.htm
[5] http://maine.gov/oit/policies/RemoteHostingPolicy.htm
[6] http://maine.gov/oit/policies/SafeguardingPolicy.htm
[7] http://maine.gov/oit/policies/waiver.htm